FIG. 1
(PRIOR ART)

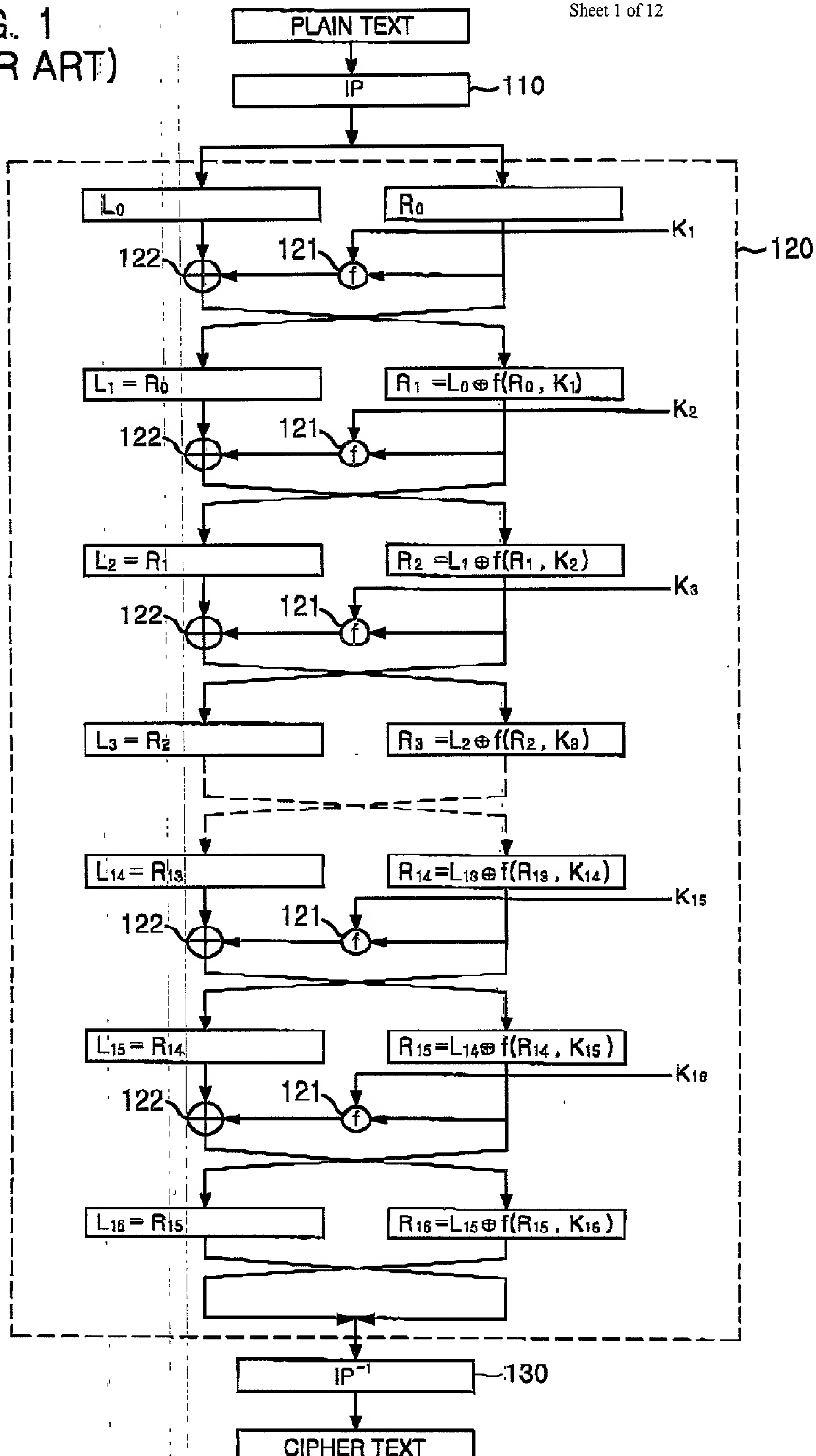


FIG. 2
(PRIOR ART)

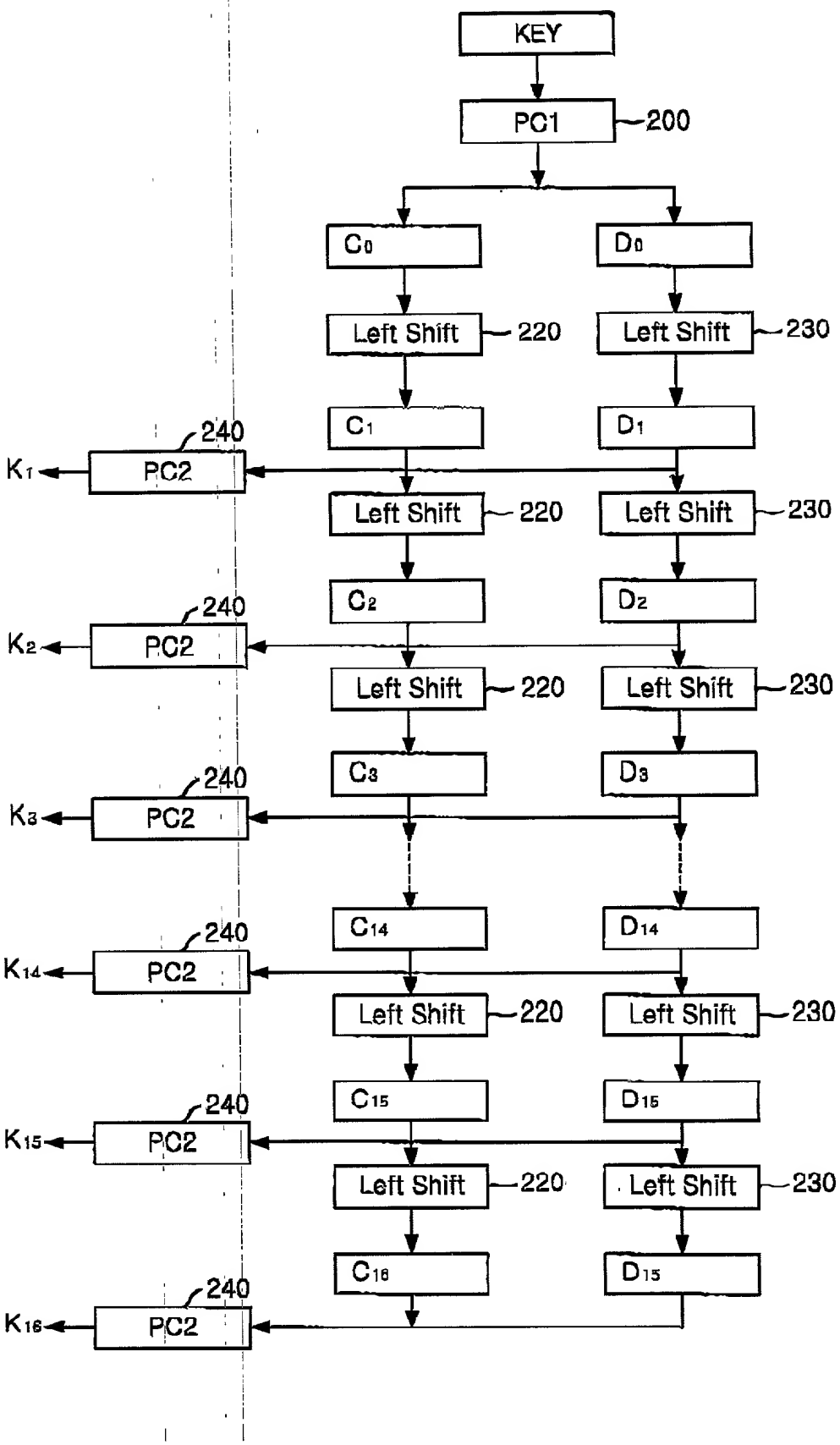


FIG. 3
(PRIOR ART)

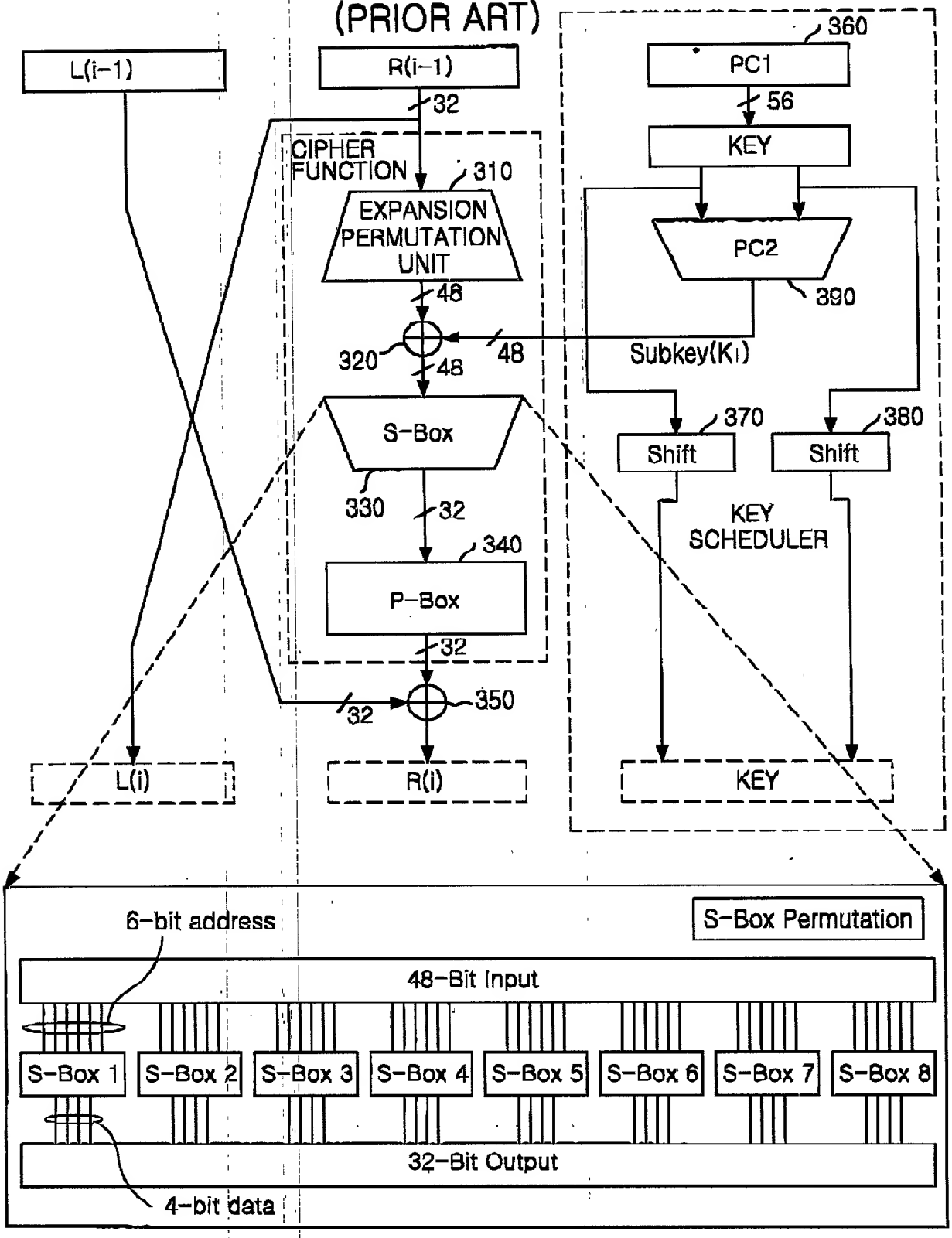
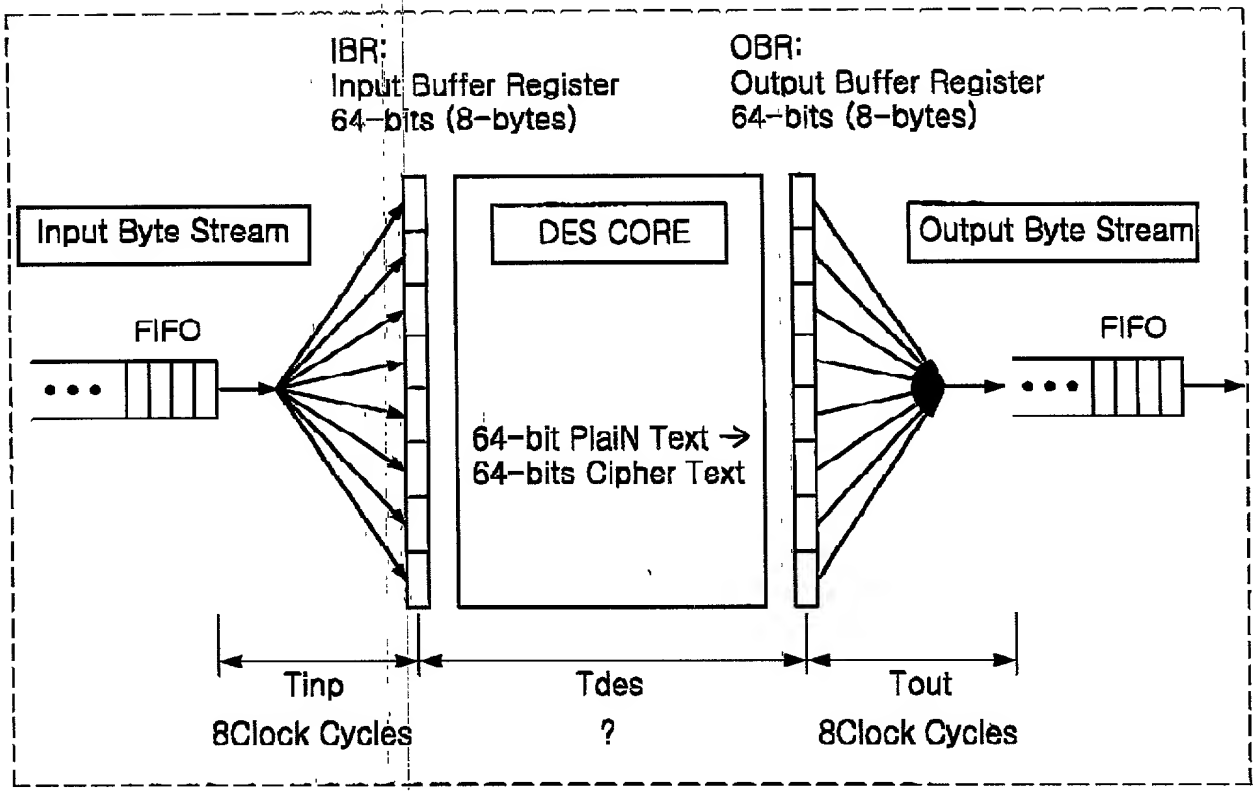


FIG. 4
(PRIOR ART)



P_i : i-th Plain Text
C_i : i-th Cipher Text
I_i : i-th Input Processing
D_i : i-th DES Processing
O_i : i-th Output Processing

Input Stage	I_0	I_1		•	•	•	I_i	•	•
DES Stage	–	D_0	D_1	D_2	•	•	D_{i-1}	•	•
Output Stage	–	–	O_0	O_1	O_2	•	O_{i-2}	•	•

P_0 P_1 P_2 • P_{i-2} P_{i-1} P_i • •

T_p

C_0 C_1 C_2 • C_{i-2} C_{i-1} C_i

=max(Tinp, Tdes, Tout)

FIG. 5A
(PRIOR ART)

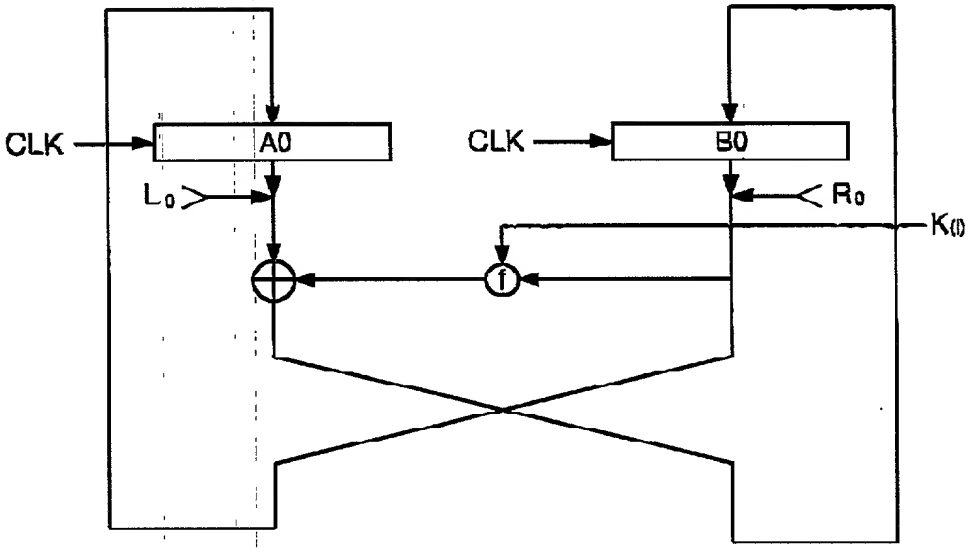
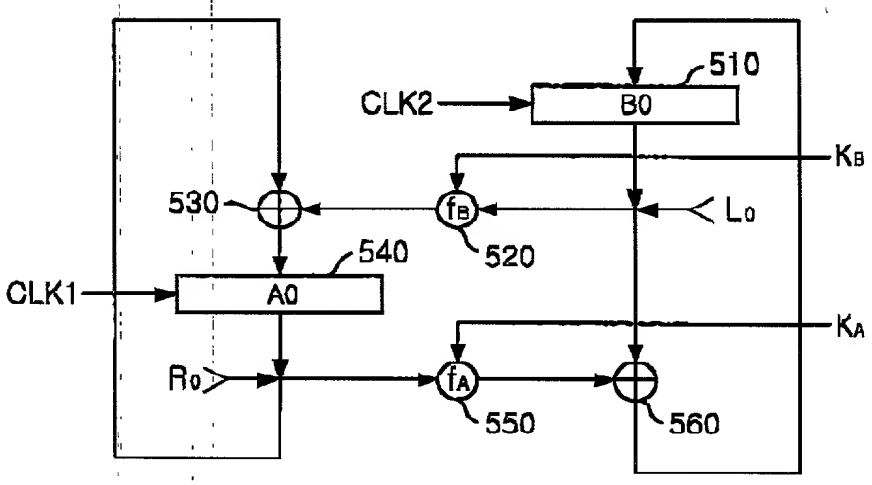


FIG. 5B



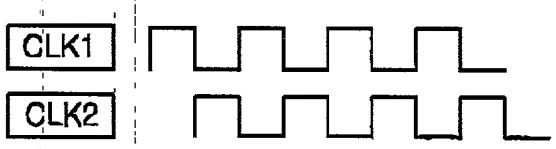


FIG. 6

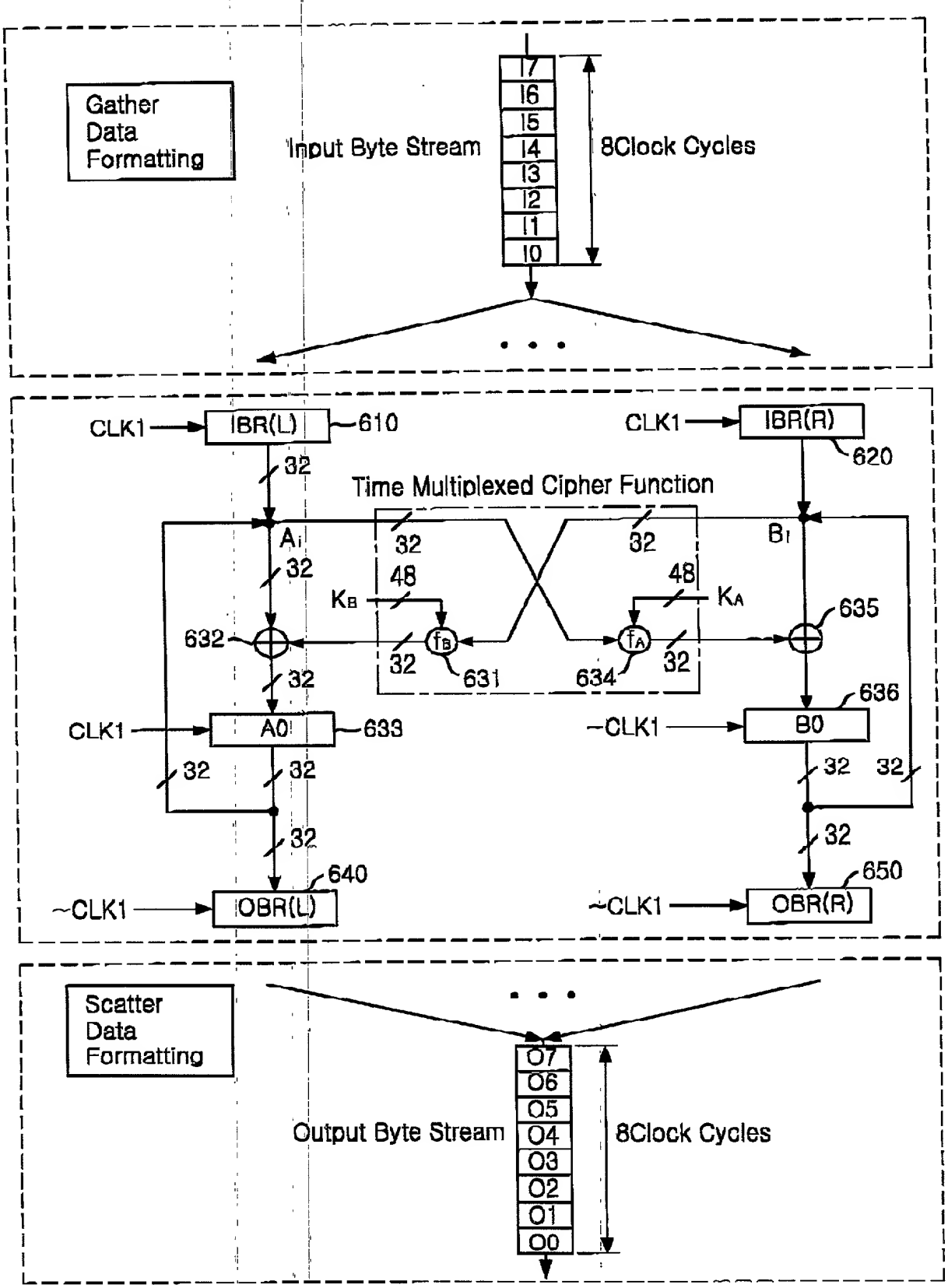

Gather Data Formatting
Input Byte Stream
I7
I6
I5
I4
I3
I2
I1
I0
8Clock Cycles
CLK1
IBR(L)
610
32
Time Multiplexed Cipher Function
Ai
32
48
KB
632
fB
631
32
CLK1
A0
633
32
32
32
640
~CLK1
OBR(L)
CLK1
IBR(R)
620
Bi
32
48
KA
635
fA
634
32
636
~CLK1
B0
32
32
32
650
~CLK1
OBR(R)
Scatter Data Formatting
Output Byte Stream
O7
O6
O5
O4
O3
O2
O1
O0
8Clock Cycles

FIG. 7

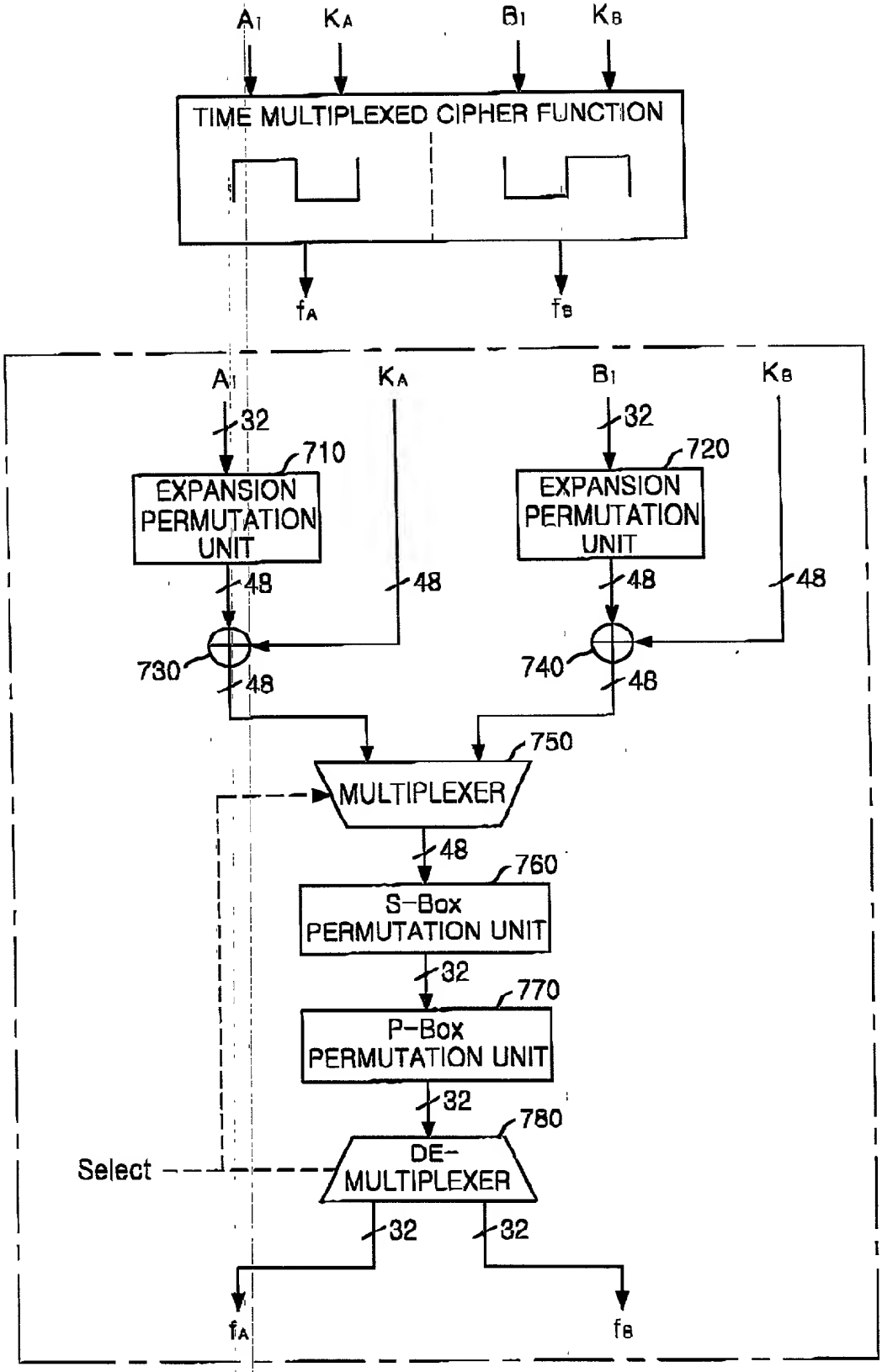

A1
KA
B1
KB
TIME MULTIPLEXED CIPHER FUNCTION
fA
fB
A1
KA
B1
KB
32
710
EXPANSION PERMUTATION UNIT
720
EXPANSION PERMUTATION UNIT
48
730
740
750
MULTIPLEXER
760
S-Box PERMUTATION UNIT
770
P-Box PERMUTATION UNIT
780
DE-MULTIPLEXER
Select

FIG. 8

Round	Left Shift Amount	Total Shift Amount
1(P_0)	3	1
2(P_1)	4	4
3(P_2)	4	8
4(P_3)	3	12
5(P_4)	4	15
6(P_5)	4	19
7(P_6)	4	23
8(P_7)	2	27

WHEN KEY IS LOADED FIRST TIME, IT SHOULD BE 1

Round	Left Shift Amount	Total Shift Amount
1(Q_0)	4	2
2(Q_1)	4	6
3(Q_2)	4	10
4(Q_3)	3	14
5(Q_4)	4	17
6(Q_5)	4	21
7(Q_6)	3	25
8(Q_7)	2	0

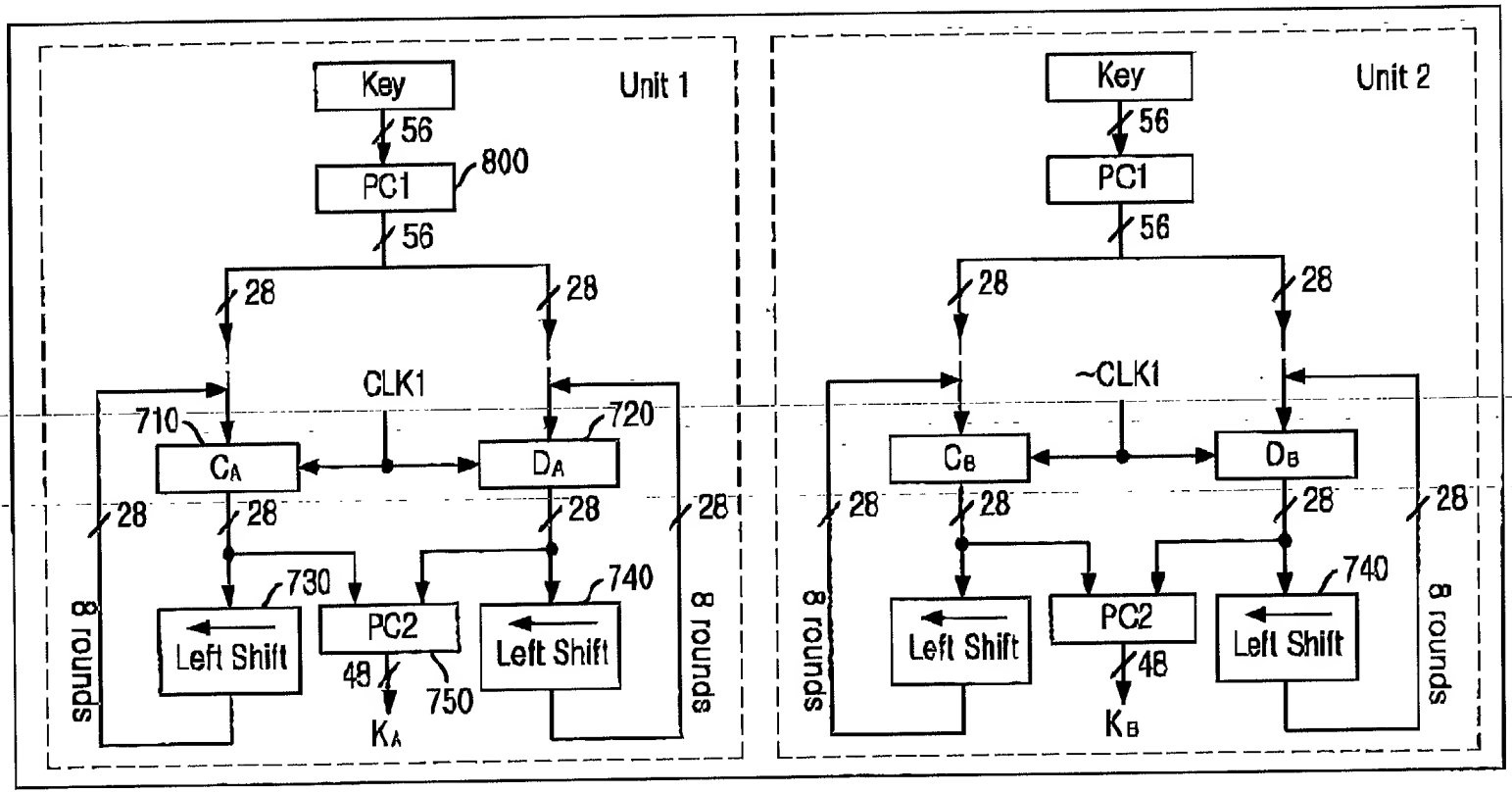


FIG. 9

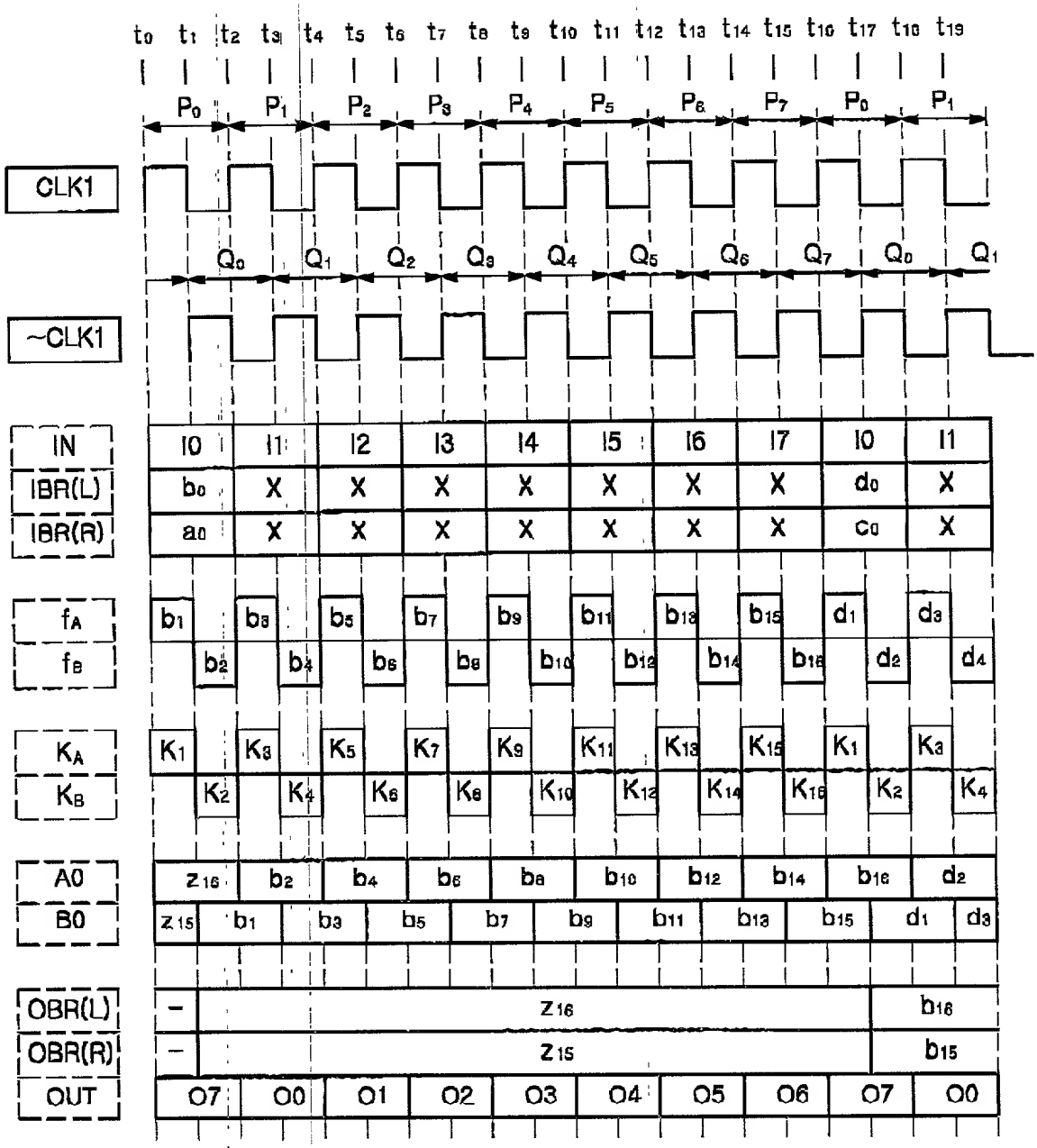

t0 t1 t2 t3 t4 t5 t6 t7 t8 t9 t10 t11 t12 t13 t14 t15 t16 t17 t18 t19
P0 P1 P2 P3 P4 P5 P6 P7 P0 P1
CLK1
Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q0 Q1
~CLK1
IN I0 I1 I2 I3 I4 I5 I6 I7 I0 I1
IBR(L) b0 X X X X X X X d0 X
IBR(R) a0 X X X X X X X c0 X
fA b1 b3 b5 b7 b9 b11 b13 b15 d1 d3
fB b2 b4 b6 b8 b10 b12 b14 b16 d2 d4
KA K1 K3 K5 K7 K9 K11 K13 K15 K1 K3
KB K2 K4 K6 K8 K10 K12 K14 K16 K2 K4
A0 z16 b2 b4 b6 b8 b10 b12 b14 b16 d2
B0 z15 b1 b3 b5 b7 b9 b11 b13 b15 d1 d3
OBR(L) – z16 b16
OBR(R) – z15 b15
OUT O7 O0 O1 O2 O3 O4 O5 O6 O7 O0

FIG. 10

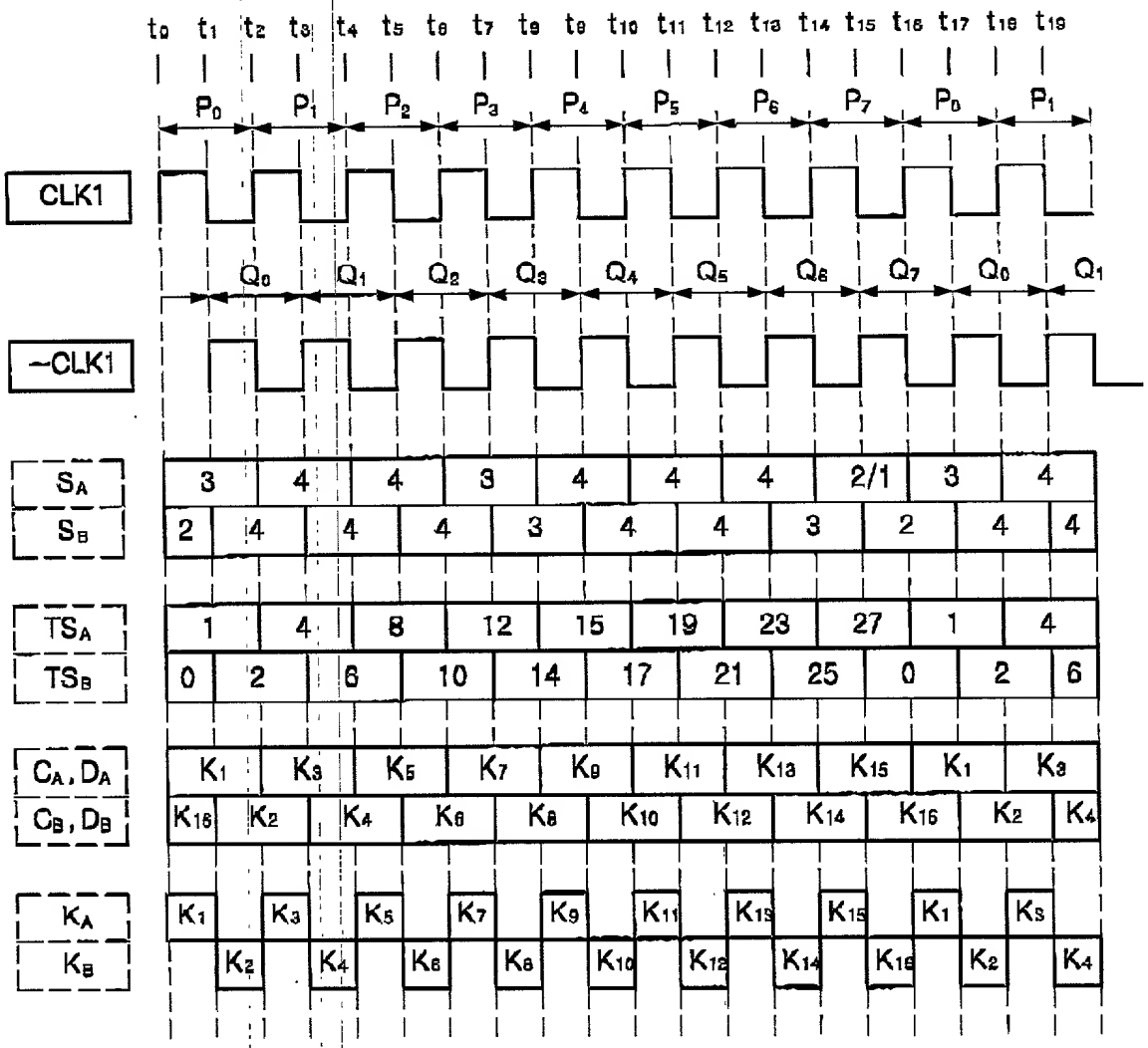

t0 t1 t2 t3 t4 t5 t6 t7 t8 t9 t10 t11 t12 t13 t14 t15 t16 t17 t18 t19
P0 P1 P2 P3 P4 P5 P6 P7 P0 P1
CLK1
Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q0 Q1
~CLK1
SA 3 4 4 3 4 4 4 2/1 3 4
SB 2 4 4 4 3 4 4 3 2 4 4
TSA 1 4 8 12 15 19 23 27 1 4
TSB 0 2 6 10 14 17 21 25 0 2 6
CA, DA K1 K3 K5 K7 K9 K11 K13 K15 K1 K3
CB, DB K16 K2 K4 K6 K8 K10 K12 K14 K16 K2 K4
KA K1 K3 K5 K7 K9 K11 K13 K15 K1 K3
KB K2 K4 K6 K8 K10 K12 K14 K16 K2 K4

FIG. 11

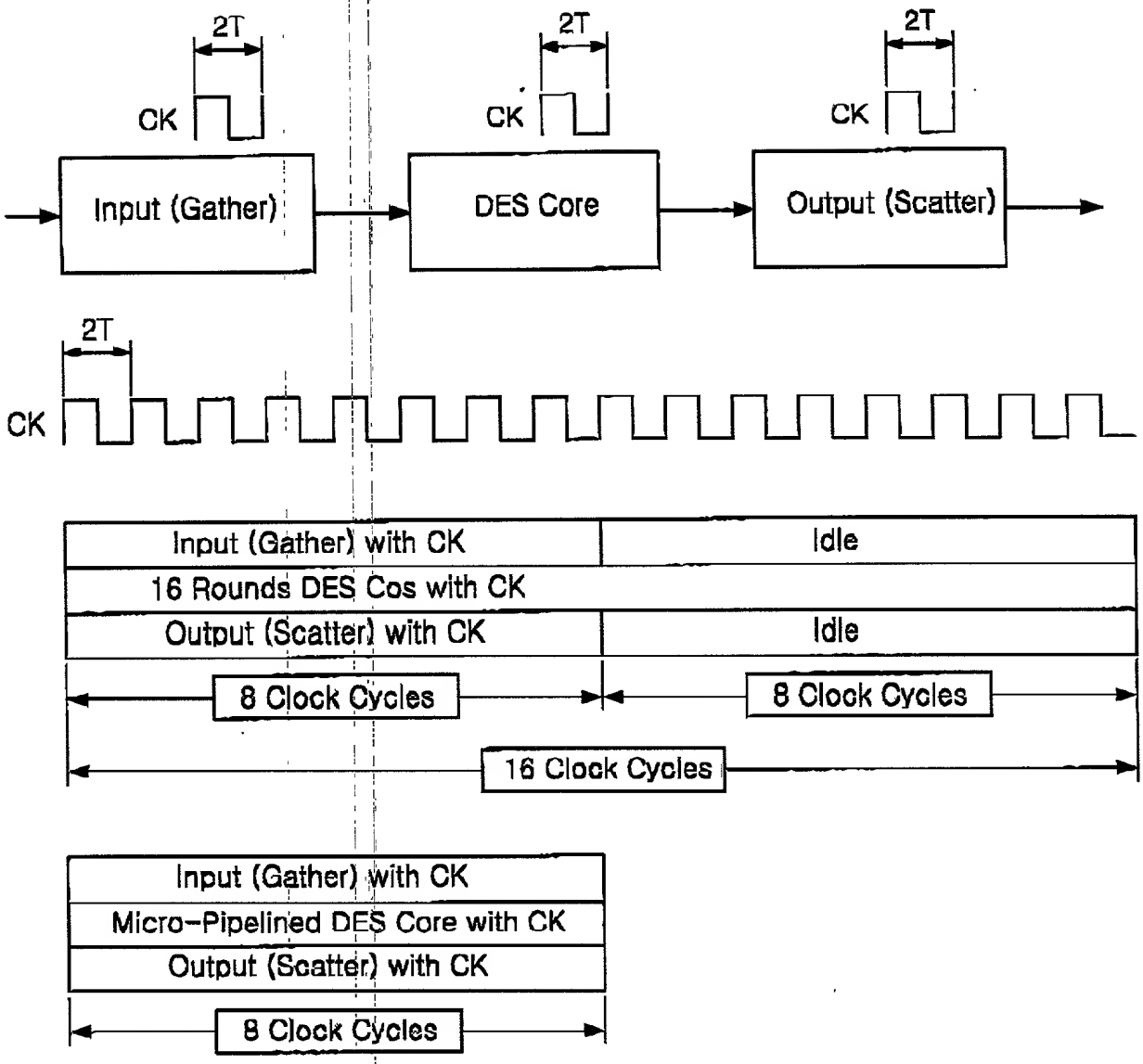
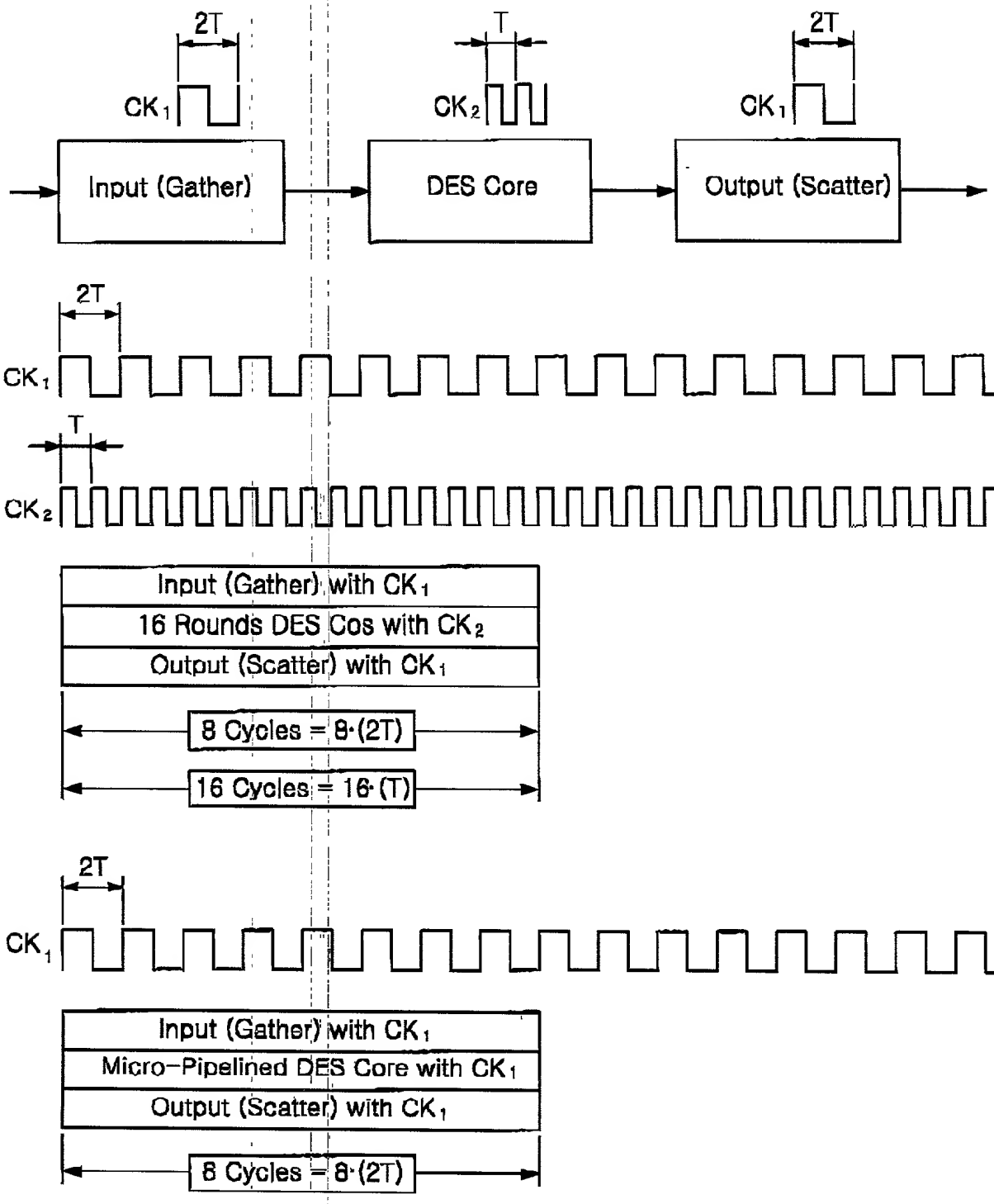

2T
CK
Input (Gather)
DES Core
Output (Scatter)
Input (Gather) with CK
Idle
16 Rounds DES Cos with CK
Output (Scatter) with CK
8 Clock Cycles
16 Clock Cycles
Micro-Pipelined DES Core with CK

FIG. 12


2T
CK1
T
CK2
2T
CK1
Input (Gather)
DES Core
Output (Scatter)
2T
CK1
T
CK2
Input (Gather) with CK1
16 Rounds DES Cos with CK2
Output (Scatter) with CK1
8 Cycles = 8·(2T)
16 Cycles = 16·(T)
2T
CK1
Input (Gather) with CK1
Micro-Pipelined DES Core with CK1
Output (Scatter) with CK1
8 Cycles = 8·(2T)